

# Concrete Security Against Adversaries with Quantum Superposition Access to Encryption and Decryption Oracles

Shahram Mossayebi and Rüdiger Schack

Royal Holloway, University of London, Egham, Surrey TW20 0EX, UK

**Abstract.** In 2013, Boneh and Zhandry introduced the notion of indistinguishability (IND) in chosen plaintext (CPA) and chosen ciphertext (CCA) attacks by a quantum adversary which is given superposition access to an oracle for encryption and decryption queries but is restricted to classical queries in the challenge phase. In this paper we define IND-CPA and IND-CCA notions for symmetric encryption schemes where the adversary has full quantum superposition access to the oracle, and give constructions that achieve these security notions. Our results are formulated in the concrete security framework.

## 1 Introduction

Even though scalable quantum computers cannot be built using current technology, the fact that they may become possible in the future has an impact on present-day information security. The relatively recent field of post-quantum cryptography [2] therefore studies classical schemes that remain secure if the adversary possesses a quantum computer. (Here and throughout the paper, “classical” is taken to mean “non-quantum”.) Since the subject of post-quantum cryptography is the security of present classical technology against future quantum attacks, the usual assumption is that only the adversary possesses quantum capabilities. This means that all communication between the adversary and the legitimate parties, in particular oracle access, is assumed to be classical.

In 2013, Boneh and Zhandry [5] went beyond this paradigm by introducing a security model in which the adversary is given quantum superposition access to encryption and decryption oracles. Their work is of considerable conceptual interest. In addition, it may become practically relevant in a future technological landscape where some cryptographic protocols are implemented on quantum computers.

Boneh and Zhandry define a notion of indistinguishability (IND) in chosen plaintext (CPA) and chosen ciphertext (CCA) attacks through a game with two phases. In the first phase (the query phase) the adversary is given unrestricted superposition oracle access. In the second phase (the challenge phase) the adversary is only allowed to make classical queries.

Why is there a restriction in the challenge phase? In their paper, Boneh and Zhandry show that some restriction is necessary. The reason is, effectively, that

a quantum computer can easily distinguish between the encryption of a single message and the encryption of an equal superposition of all possible messages, independently of the details of the encryption. The restriction to classical challenge queries prevents the adversary to exploit this fact and allows Boneh and Zhandry to prove that their security notion is achievable. It is worth pointing out that even in standard (classical) indistinguishability notions it is necessary to restrict the class of allowed challenge queries, to prevent the adversary from winning the game trivially by exploiting information about, e.g., message length.

There is a sense, however, in which a restriction to classical challenge queries seems too strong. Considering quantum oracle access makes sense only in view of a future technological environment in which the legitimate parties use quantum computers. In such an environment, it is likely that the encryption schemes considered here will form part of a wider quantum communication infrastructure. Without a precise specification of the nature of this infrastructure, one should not rule out a priori the possibility that an adversary might benefit from the ability to distinguish between superpositions of messages or ciphertexts.

In this paper we introduce an achievable security notion where the adversary has full superposition access to an oracle. We define an indistinguishability (IND) notion in both chosen plaintext (CPA) and chosen ciphertext (CCA) attacks. Our IND notion, which we call “real or permutation” (RoP), is equivalent to standard IND notions in the case of classical oracle queries, but is immune to the attack discovered by Boneh and Zhandry in the case of quantum superposition queries. It also falls outside the classification of security notions recently given by Gagliardoni, Hülsing and Schaffner [6]. It would be worthwhile to study the relationship between our CPA notion and the qIND-qCPA notion defined in [6]. Whereas we consider direct quantum-mechanical interaction between adversary and oracle, qIND-qCPA requires the adversary to submit classical descriptions of its quantum queries.

In a RoP experiment, the adversary is given access to one of two encryption oracles. One oracle simply encrypts challenge messages chosen by the adversary, whereas the other oracle applies a random permutation to the message and then encrypts it. The adversary’s goal is to distinguish between the two cases. For classical queries, applying a random permutation to a message is equivalent to replacing the message by a random string. For classical queries, the RoP security notion is therefore equivalent to the “real or random” notion defined in [3]. In the quantum case, the RoP notion allows for arbitrary quantum superposition queries in all phases of the experiment.

The paper is organized as follows. In Section 2 we describe our security model, for which we adopt the concrete-security paradigm [3]. Section 3 discusses quantum pseudorandom functions (QPRF) and their existence from the concrete-security standpoint. In Section 4 we define our real or permutation IND-CPA notion and show that it is achieved by a slight modification of a standard construction. The CCA case is the topic of Section 5. The proof that the RoP IND-CCA notion is achievable is the main contribution of this paper. The proof contains new ideas and substantial input from quantum information theory.

## 2 Security Model

In this paper we address the security of symmetric encryption schemes against quantum adversaries [8,11]. We adopt the usual definition of a symmetric encryption scheme as a triple  $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$  consisting of a (randomized) key generation algorithm  $\mathcal{K}$ , a (randomized) encryption algorithm that takes a plaintext  $M$  and a key  $K$  and returns a ciphertext  $C = \mathcal{E}_K(M)$ , and a decryption algorithm satisfying  $\mathcal{D}_K(\mathcal{E}_K(M)) = M$  for all messages  $M$ . We assume that  $\mathcal{E}$  is randomized, i.e., its output depends on a string  $r$  which is chosen randomly each time  $\mathcal{E}$  is invoked.

We will consider both chosen plaintext attacks (CPA), where an adversary is given access to an encryption oracle, and chosen ciphertext attacks (CCA), where the adversary in addition has access to a decryption oracle. We will assume that both  $\mathcal{E}$  and  $\mathcal{D}$  are implemented on a quantum computer [10], and that the adversary is given superposition access to the corresponding oracles. By this we mean, roughly, that the adversary can make encryption queries consisting of quantum superpositions of messages, to which the oracle responds with a corresponding superposition of ciphertexts, and similarly for decryption queries in the CCA case.

Formally we define a superposition query as follows. For any function  $f : \{0,1\}^n \rightarrow \{0,1\}^m$  we define a unitary transformation,  $\mathbf{U}_f$ , on a  $(n+m)$ -qubit register by

$$\mathbf{U}_f|x, y\rangle = |x, y \oplus f(x)\rangle, \quad (1)$$

where  $x$  is an  $n$ -bit string,  $y$  is an  $m$ -bit string, and

$$|x, y\rangle = |x\rangle|y\rangle = |x\rangle \otimes |y\rangle, \quad (2)$$

the *computational basis states*, form an orthonormal basis of  $2^{n+m}$ -dimensional complex Hilbert space. Equation (1) defines the action of  $\mathbf{U}_f$  for arbitrary quantum states on the quantum register, including superposition states and including the case that the register is entangled with some other quantum register.

In this scenario, an encryption query consists in the application of the unitary  $\mathbf{U}_{\mathcal{E}_K}$  to a quantum register under the control of the adversary, and similarly for a decryption query. We place no restrictions on the initial state of the adversary's register. If the initial state is of the superposition form  $|\psi\rangle = \sum_M c_M |M, 0\rangle$  with arbitrary complex coefficients  $c_M$ , the result of the query is

$$\mathbf{U}_{\mathcal{E}_K}|\psi\rangle = \sum_M c_M |M, \mathcal{E}_K(M)\rangle. \quad (3)$$

The resources required to apply the unitary  $\mathbf{U}_{\mathcal{E}_K}$  to a quantum register are independent of the initial state  $|\psi\rangle$  of the register. Applying a unitary can be thought of as a single physical operation, for which the number of terms in the superposition state  $|\psi\rangle$  is irrelevant. Since the encryption oracle does not “know” whether it acts on a superposition or on a single basis state, we will assume that the random string  $r$  required for the randomized encryption is chosen exactly

once every time  $\mathbf{U}_{\mathcal{E}_K}$  is applied. This means that  $r$  is the same for all terms in the sum in Eq. (3).

In the most general definition, a *quantum adversary*  $\mathcal{A}$  is a quantum algorithm that runs on a quantum computer. In this paper, we will assume that  $\mathcal{A}$  takes an (optional) bit string  $i$  as input, has access to one or more oracles  $f_1, f_2, \dots$  and eventually halts, outputting a bit string  $o$ . We will denote this process by

$$o \leftarrow \mathcal{A}^{f_1, f_2, \dots}(i) . \quad (4)$$

We will assume that  $\mathcal{A}$  maintains a quantum register  $Q_{\mathcal{A}}$  for the purpose of making oracle queries, a quantum register  $S_{\mathcal{A}}$  for doing quantum computations and for storing its internal state between invocations, and a register  $R_{\mathcal{A}}$  for classical input and output. Passing an argument  $i$  to  $\mathcal{A}$  is done by placing  $i$  into the register  $R_{\mathcal{A}}$ . One could model  $R_{\mathcal{A}}$  as a quantum register, but in practice one would expect quantum algorithms to have classical as well as quantum parts. Whenever  $\mathcal{A}$  makes a query to an oracle  $f$ , the unitary operation  $U_f$  defined in Eq. (1) is applied to the register  $Q_{\mathcal{A}}$ . Since it is implicit in Eq. (1) that  $U_f$  is applied to  $n + m$  qubits, we will assume that  $\mathcal{A}$  puts the parameters  $n$  and  $m$  in the register  $R_{\mathcal{A}}$  if there is any ambiguity.

In this paper we adopt the concrete security framework [3]. Instead of focusing on polynomial algorithms in an asymptotic sense, concrete security concerns bounds on an adversary’s success probability as a function of the actual resources available to the adversary.

The most relevant resources for the purposes of this paper are the running time of a quantum adversary  $\mathcal{A}$ , and the number of oracle queries made by  $\mathcal{A}$ . We define the running time as the time, in seconds, that elapses until  $\mathcal{A}$  writes its final output and halts, including any initialization steps. There exist a number of further potentially important resource parameters, such as memory size, or the number of qubits required by  $\mathcal{A}$ , but since these do not play any explicit role in the reduction arguments given below, we will not discuss them here.

Our reduction arguments can be read in a very “concrete” way, e.g., “if there exists a specific quantum adversary that, in  $10^4$  seconds and using  $10^9$  oracle queries achieves an advantage of  $2 \times 10^{-2}$  in an attack on scheme  $X$ , then one can construct another quantum adversary that, also in  $10^4$  seconds and using  $10^9$  oracles queries, achieves an advantage of at least  $10^{-2}$  in an attack on scheme  $Y$ .” Working within the concrete-security paradigm and measuring running time in seconds rather than as the number of, say, gate operations has the clear advantage that it leads to definitions and theorems which are independent of any particular computing or quantum computing model.

### 3 Quantum pseudorandom functions

In a concrete security framework, a quantum pseudorandom function, or QPRF, is simply a family of functions. What turns a family of functions into a QPRF is a pair of experiments that defines an adversary’s *QPRF advantage*.

$\mathbf{Exp}_F^{\text{qprf}-0}(\mathcal{A})$	$\mathbf{Exp}_F^{\text{qprf}-1}(\mathcal{A})$
$K \leftarrow \mathcal{K}$	$f \leftarrow \text{Func}(\mathcal{X}, \mathcal{Y})$
$b \leftarrow \mathcal{A}^{F_K}$	$b \leftarrow \mathcal{A}^f$
<b>return</b> $b$	<b>return</b> $b$

**Fig. 1.** The two experiments defining a QPRF.

So let  $F : \mathcal{K} \times \mathcal{X} \rightarrow \mathcal{Y}$  be a function family identified by the set  $\mathcal{K}$ . Consider two oracles: one formed by an instance  $F_K = F(K, \cdot)$  for a random  $K \in \mathcal{K}$ , the other given by a function  $f$  chosen randomly from the set  $\text{Func}(\mathcal{X}, \mathcal{Y})$  of functions from  $\mathcal{X}$  to  $\mathcal{Y}$ . The QPRF advantage is a measure of the adversary's ability to distinguish an instance drawn from the function family from a function chosen at random from  $\text{Func}(\mathcal{X}, \mathcal{Y})$ .

**Definition 1 (QPRF).** Define experiments  $\mathbf{Exp}_F^{\text{qprf}-0}$  and  $\mathbf{Exp}_F^{\text{qprf}-1}$  as in Figure 1. In both experiments, the quantum adversary  $\mathcal{A}$  is given access to an oracle and eventually outputs a bit,  $b$ . In  $\mathbf{Exp}_F^{\text{qprf}-0}$ , a key  $K \in \mathcal{K}$  is chosen at random and the adversary's oracle queries are answered by applying the unitary operator  $\mathbf{U}_{F_K}$  to the adversary's register  $Q_{\mathcal{A}}$ . In  $\mathbf{Exp}_F^{\text{qprf}-1}$ , a function  $f \in \text{Func}(\mathcal{X}, \mathcal{Y})$  is chosen at random and the adversary's oracle queries are answered by similarly applying the unitary operator  $\mathbf{U}_f$ . The QPRF advantage of  $\mathcal{A}$  is defined as

$$\mathbf{Adv}_F^{\text{qprf}}(\mathcal{A}) = \Pr \left[ \mathbf{Exp}_F^{\text{qprf}-1}(\mathcal{A}) = 1 \right] - \Pr \left[ \mathbf{Exp}_F^{\text{qprf}-0}(\mathcal{A}) = 1 \right].$$

In the next two sections, we will analyze the security of encryption schemes which are based on a QPRF. For these schemes to be secure, we need to assume that there exists a function family  $F$  such that its QPRF-advantage is extremely small for any quantum adversary using resources that are available now or might become available in the foreseeable future. Such function families are widely believed to exist in the form of standard block ciphers, for instance AES-256. The best currently known quantum attack against AES-256 uses Grover's search algorithm [7,10] and requires of the order of  $2^{128}$  queries to find the encryption key with high probability. The security of the schemes discussed below depends on the heuristic assumption that AES-256 or similar block ciphers cannot be broken by a quantum computer using realistic resources.

## 4 Quantum Superposition Chosen Plaintext Attack

To define indistinguishability in a CPA attack for a symmetric encryption scheme  $\mathcal{SE}$ , we introduce a pair of experiments as in Figure 2. We call them real or permutation, or RoP, experiments, in analogy to the real or random notion defined in [3]. In each experiment, the quantum adversary is given superposition access to an encryption oracle. The encryption oracle responds to each encryption query by applying a unitary transformation to the adversary's quantum register

```

Exp $\mathcal{SE}$  $rop-qscpa-b$ ( $\mathcal{A}$ )
   $K \leftarrow \$ \mathcal{K}$ 
   $b' \leftarrow \$ \mathcal{A}^{\text{RoP}_{Q_{\mathcal{A}}}(\cdot)}$ 
  return  $b'$ 

RoP $Q_{\mathcal{A}}$ ( $\cdot$ )
  if  $b = 1$  then
    Apply  $\mathbf{U}_{\mathcal{E}_K(\cdot)}$  to  $Q_{\mathcal{A}}$ 
  else
     $\Pi \leftarrow \$ \text{Perm}(n)$ 
    Apply  $\mathbf{U}_{\Pi(\cdot)}$  to  $Q_{\mathcal{A}}$ 
    Apply  $\mathbf{U}_{\mathcal{E}_K(\cdot)}$  to  $Q_{\mathcal{A}}$ 
  end if
  return

```

**Fig. 2.** The RoP-qscPA confidentiality notion

$Q_{\mathcal{A}}$ . The transformation depends on the bit  $b$ . If  $b = 1$ , the transformation is given by

$$|m, x\rangle \longrightarrow |m, x \oplus \mathcal{E}_K(m)\rangle, \quad (5)$$

and if  $b = 0$ , it is

$$|m, x\rangle \longrightarrow |m, x \oplus \mathcal{E}_K(\Pi(m))\rangle, \quad (6)$$

where  $\Pi$  is a permutation chosen uniformly at random. This means that in the case  $b = 0$ , before the encryption a random permutation is applied to each term in the superposition of plaintexts. The goal of the quantum adversary is to distinguish between the two experiments.

**Definition 2 (RoP-qscPA).** Let  $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$  be a symmetric encryption scheme. Define experiment  $\mathbf{Exp}_{\mathcal{SE}}^{rop-qscpa-b}(\mathcal{A})$  for a quantum adversary  $\mathcal{A}$  and a bit  $b$  as shown in Figure 2. In the experiment, the adversary  $\mathcal{A}$  is given quantum superposition access to a real-or-permutation encryption oracle  $\text{RoP}_{Q_{\mathcal{A}}}(\cdot)$ . The encryption oracle responds to each query by applying a unitary transformation to the adversary's quantum register  $Q_{\mathcal{A}}$ .

The adversary's goal is to output a bit  $b'$  as its guess of the challenge bit  $b$ , and the experiment returns  $b'$  as well. The advantage of  $\mathcal{A}$  is given by:

$$\mathbf{Adv}_{\mathcal{SE}}^{rop-qscpa}(\mathcal{A}) = \Pr \left[ \mathbf{Exp}_{\mathcal{SE}}^{rop-qscpa-1}(\mathcal{A}) = 1 \right] - \Pr \left[ \mathbf{Exp}_{\mathcal{SE}}^{rop-qscpa-0}(\mathcal{A}) = 1 \right].$$

This advantage refers to a specific quantum adversary using resources as defined in Section 2.  $\square$

We now show that the above RoP-qscPA indistinguishability notion can be achieved. To motivate our construction, we first show that the following standard construction (see, e.g., [9]) is insecure with respect to our notion :

**Construction 1’:** Let  $F$  be a QPRF. The following construction defines a symmetric encryption scheme  $\mathcal{SE} = (\mathcal{E}, \mathcal{D})$ :

$$\begin{aligned} \mathcal{E}(K, m) : & \quad r \leftarrow \$ \{0, 1\}^* \\ & \quad c \leftarrow F_K(r) \oplus m \\ & \quad \textbf{output} \ (r, c) \\ \mathcal{D}(K, r, c) : & \quad m \leftarrow F_K(r) \oplus c \\ & \quad \textbf{output} \ (m) \end{aligned}$$

Suppose the state  $\mathcal{N} \sum_m |0, m\rangle$  is submitted to the encryption oracle, where  $\mathcal{N}$  is a normalization constant. In the “real case” ( $b = 1$ ), the result is the state  $\mathcal{N} \sum_m |m, m \oplus y\rangle$ , where  $y = F_K(r)$ . In the “permutation” case ( $b = 0$ ), the result is the state  $\mathcal{N} \sum_m |m, \Pi(m \oplus y)\rangle$ . A Fourier transform followed by a measurement will distinguish these two states with probability almost 1.

The problem is that the same randomness  $r$  is used for all terms in the superposition. The following modified construction overcomes this problem.

**Construction 1:** Let  $F$  be a QPRF. The following construction defines a symmetric encryption scheme  $\mathcal{SE} = (\mathcal{E}, \mathcal{D})$ :

$$\begin{aligned} \mathcal{E}(K, m) : & \quad r \leftarrow \$ \{0, 1\}^* \\ & \quad s \leftarrow F_r(m) \\ & \quad c \leftarrow F_K(s) \oplus m \\ & \quad \textbf{output} \ (s, c) \\ \mathcal{D}(K, s, c) : & \quad m \leftarrow F_K(s) \oplus c \\ & \quad \textbf{output} \ (m) \end{aligned}$$

To prove that the modified construction achieves our notion of RoP-qSCPA security, we are going to provide a straightforward reduction proof. In the concrete security framework adopted here this means that, if the above construction can be broken by a specific quantum adversary, the reduction establishes the existence of a quantum adversary using similar resources that breaks the underlying QPRF. But as we saw in Section 3, a QPRF based on a suitably chosen block cipher is currently thought to be secure against quantum attacks.

**Theorem 1 (RoP-qSCPA security is achievable).** *Let  $\mathcal{A}$  be a quantum adversary attacking the encryption scheme  $\mathcal{SE}$ , based on a QPRF  $F$  as in Construction 1, in the RoP-qSCPA sense. Assume  $\mathcal{A}$  makes at most  $q$  queries to the encryption oracle and has advantage*

$$\text{Adv}_{\mathcal{SE}}^{\text{rop-qscpa}}(\mathcal{A}) \geq \epsilon .$$

*Then there exists a quantum adversary  $\mathcal{B}$  attacking  $F$ , making at most  $q$  queries to the encryption oracle and having advantage*

$$\text{Adv}_F^{\text{qprf}}(\mathcal{B}) \geq \frac{\epsilon}{2(q+1)} .$$

**Proof.** To prove the theorem one (i) establishes the security of the scheme when  $F$  is replaced by a truly random function  $f$ . Then (ii) one shows that, if the scheme is insecure when the QPRF  $F$  is used, then there exists a quantum adversary which can distinguish  $F$  from a truly random function and thus breaks  $F$ .

For part (i), assume that in Construction 1, the QPRF  $F_K$  is replaced by a random function  $g$ , and in the  $j$ -th invocation of the encryption oracle ( $j = 1, \dots, q$ ), the QPRF  $F_r$  is replaced by a random function  $f_j$ . Assume that the length of  $s$  is chosen so large that computing  $f_j(m)$  for all  $m$  and  $j$  leads to collisions with exponentially small probability. For simplicity we assume that the same QPRF is used throughout, if necessary by padding keys and/or arguments. No collisions means that for all  $m_1, m_2$  in the message space and for all  $i, j$ ,  $f_i(m_1) = f_j(m_2) \Rightarrow i = j$  and  $m_1 = m_2$ . Then  $g(f_j(m))$  for all  $m$  and  $j$  are independent random strings. Therefore the set  $\{(f_j(m), g(f_j(m)) \oplus m)\}$  is information-theoretically indistinguishable from the set  $\{(f_j(m), g(f_j(m)) \oplus \Pi(m))\}$ . It follows that having access to superpositions of states from the one or the other set cannot give rise to a positive advantage.

The above argument relies on the fact that information-theoretic notions carry over to the quantum case. This is the only quantum argument needed in this proof. Part (ii) of the proof proceeds by a standard hybrid argument that assumes only classical queries. It is therefore omitted here.

## 5 Quantum Superposition Chosen Ciphertext Attack

In a CCA attack against a symmetric encryption scheme  $\mathcal{SE}$  the quantum adversary is given, in addition to an encryption oracle as in the CPA case, superposition access to a decryption oracle. To define indistinguishability in this case, we introduce the pair of experiments in Figure 3. The decryption oracle responds to each decryption query by applying the following unitary transformation to the quantum adversary's register  $Q_A$ :

$$|x, c\rangle \longrightarrow |x \oplus \mathcal{D}_K(c), c\rangle. \quad (7)$$

To arrive at a meaningful definition, we have to exclude decryption queries consisting in the results of encryption queries.

**Definition 3 (RoP-qSCCA).** Let  $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$  be a symmetric encryption scheme. Define experiment  $\mathbf{Exp}_{\mathcal{SE}}^{\text{rop-qscqa}-b}(\mathcal{A})$  for a quantum adversary  $\mathcal{A}$  and a bit  $b$  as in Figure 3. In the experiment, the adversary  $\mathcal{A}$  is given quantum superposition access to a real-or-permutation encryption oracle  $\text{RoP}_{Q_A}()$  as well as a decryption oracle,  $\text{Dec}_{Q_A}()$ .

Now denote by  $\rho_i^e$  the state of the register  $Q_A$  directly after the  $i$ -th encryption query, and by  $\rho_j^d$  the state of the register directly before the  $j$ -th decryption query. For any (classical) ciphertext  $c$  that occurs as the result of an encryption query, i.e., for any ciphertext  $c$  such that  $\langle c | \rho_i^e | c \rangle \neq 0$  for some  $i$ , we require  $\langle c | \rho_j^d | c \rangle = 0$  for all  $j$ .



```

 $\mathbf{Exp}_{\mathcal{SE}}^{rop-qcca-b}(\mathcal{A})$ 
     $K \leftarrow \mathcal{K}$ 
     $b' \leftarrow \mathcal{A}^{\text{RoP}_{Q_{\mathcal{A}}}(\cdot), \text{Dec}_{Q_{\mathcal{A}}}(\cdot)}$ 
    return  $b'$ 

 $\text{RoP}_{Q_{\mathcal{A}}}(\cdot)$ 
    if  $b = 1$  then
        Apply  $\mathbf{U}_{\mathcal{E}_K(\cdot)}$  to  $Q_{\mathcal{A}}$ 
    else
         $\Pi \leftarrow \$\text{Perm}(n)$ 
        Apply  $\mathbf{U}_{\Pi(\cdot)}$  to  $Q_{\mathcal{A}}$ 
        Apply  $\mathbf{U}_{\mathcal{E}_K(\cdot)}$  to  $Q_{\mathcal{A}}$ 
    end if
    return

 $\text{Dec}_{Q_{\mathcal{A}}}(\cdot)$ 
    Apply  $\mathbf{U}_{\mathcal{D}_K(\cdot)}$  to  $Q_{\mathcal{A}}$ 
    return

```

**Fig. 3.** The RoP-qSCCA confidentiality notion

The adversary's goal is to output a bit  $b'$  as its guess of the challenge bit  $b$ , and the experiment returns  $b'$  as well. The advantage of  $\mathcal{A}$  is given by

$$\mathbf{Adv}_{\mathcal{SE}}^{rop-qcca}(\mathcal{A}) = \Pr \left[ \mathbf{Exp}_{\mathcal{SE}}^{rop-qcca-1}(\mathcal{A}) = 1 \right] - \Pr \left[ \mathbf{Exp}_{\mathcal{SE}}^{rop-qcca-0}(\mathcal{A}) = 1 \right].$$

This advantage refers to a specific quantum adversary using resources as defined in Section 2.  $\square$

The restriction on the adversary's decryption queries could be made less restrictive by replacing the condition  $\langle c | \rho_j^d | c \rangle = 0$  by  $\langle c | \rho_j^d | c \rangle < \delta$  for some  $\delta > 0$ . The complication entailed by this did not, however, seem justified as, due to the randomization, the ciphertext space is much larger than the message space. It is worth pointing out it cannot be checked even in principle whether the adversary honors the restriction on its decryption queries. This is because, in a superposition query, the oracle (or experiment) can have no information on what messages or ciphertexts are submitted as part of the query.

We now show that the above indistinguishability notion can be achieved by the following standard Encrypt-then-MAC construction [4]:

**Construction 2:** Let  $\mathcal{SE} = (\mathcal{E}, \mathcal{D})$  be a symmetric encryption scheme and let  $F$  be a QPRF. The following construction defines a symmetric encryption scheme

$\mathcal{SE}' = (\mathcal{E}', \mathcal{D}')$ :

$$\begin{aligned} \mathcal{E}'((K_1, K_2), m) : & \quad c \leftarrow \mathcal{E}_{K_1}(m), \tau \leftarrow F_{K_2}(c) \\ & \quad \textbf{output } (c, \tau) \\ \mathcal{D}'((K_1, K_2), c, \tau) : & \quad \tau' \leftarrow F_{K_2}(c), m \leftarrow \mathcal{D}_{K_1}(c) \\ & \quad \textbf{if } \tau = \tau', \textbf{ output } (m) \\ & \quad \textbf{otherwise, output } \perp \end{aligned}$$

The symbol  $\perp$  denotes some fixed string that is outside the message space. The decryption returns  $\perp$  if the tag is invalid. A quantum decryption oracle is described by a unitary operator  $\mathbf{V}$  acting on a register state  $|x, c, \tau\rangle$  as follows:

$$\mathbf{V}|x, c, \tau\rangle = \begin{cases} |x \oplus \mathcal{D}_{K_1}(c), c, \tau\rangle & \text{if } F_{K_2}(c) = \tau, \\ |x \oplus \perp, c, \tau\rangle & \text{otherwise.} \end{cases} \quad (8)$$

The following theorem establishes that, if the above construction can be broken by a specific quantum adversary, then there exist quantum adversaries using similar resources that break the underlying QPRF or the RoP-qSCPA security of the underlying scheme  $\mathcal{SE}$ . But as we saw in Sections 3 and 4, a QPRF based on a suitably chosen block cipher is currently thought to be secure against quantum attacks, and RoP-qSCPA security is achievable.

**Theorem 2 (RoP-qSCCA security is achievable).** *Consider the scheme  $\mathcal{SE}'$  in Construction 2 based on a QPRF  $F$  and an encryption scheme  $\mathcal{SE}$ . Assume  $\mathcal{A}$  is a quantum adversary attacking  $\mathcal{SE}'$  in the RoP-qSCCA sense, making at most  $q_e$  encryption and  $q_d$  decryption queries to the oracle, and having advantage*

$$\text{Adv}_{\mathcal{SE}'}^{\text{rop-qscca}}(\mathcal{A}) \geq \epsilon.$$

*Then there exist quantum adversaries  $\mathcal{B}$  and  $\mathcal{J}$  attacking  $\mathcal{SE}$  and  $F$  respectively, as follows.  $\mathcal{B}$  makes at most  $q_e$  encryption oracle queries.  $\mathcal{J}$  makes at most  $q_d$  oracle queries. The advantages satisfy*

$$\text{Adv}_{\mathcal{SE}}^{\text{rop-qscpa}}(\mathcal{B}) + 2 \cdot \text{Adv}_F^{\text{qprf}}(\mathcal{J}) \geq \epsilon - 2(1 + 2q_d^2)2^{-n_\tau/4},$$

where  $n_\tau$  is the length of the tag  $\tau$  as defined in Construction 2.

*Proof.* As in the proof of Theorem 1, we first modify Construction 2 by replacing  $F$  with a true random function  $f$ . We then show, roughly, (i) that a quantum adversary that can distinguish between these two constructions can break the QPRF security of  $F$ , and (ii) that a quantum adversary that breaks the modified construction can break the CPA security of the underlying scheme  $\mathcal{SE}$ .

We denote the modified scheme by  $\tilde{\mathcal{SE}} = (\tilde{\mathcal{E}}, \tilde{\mathcal{D}})$ :

$$\begin{aligned} \tilde{\mathcal{E}}(K_1, m) : & \quad c \leftarrow \mathcal{E}_{K_1}(m), \tau \leftarrow f(c) \\ & \quad \textbf{output } (c, \tau) \\ \tilde{\mathcal{D}}(K_1, c, \tau) : & \quad \tau' \leftarrow f(c), m \leftarrow \mathcal{D}_{K_1}(c) \\ & \quad \textbf{if } \tau = \tau', \textbf{ output } (m) \\ & \quad \textbf{otherwise, output } \perp \end{aligned}$$

Here,  $f$  is a function chosen uniformly at random.

Now let  $\mathcal{A}$  be a quantum adversary attacking the CCA security of  $\mathcal{SE}'$ . A standard argument [9] then leads to the construction of a quantum adversary  $\mathcal{J}$  attacking the QPRF  $F$ , making  $q_d$  oracles queries and having advantage

$$\mathbf{Adv}_F^{qprf}(\mathcal{J}) \geq \frac{1}{2} \mathbf{Adv}_{\mathcal{SE}'}^{rop-qcca}(\mathcal{A}) - \frac{1}{2} \mathbf{Adv}_{\widetilde{\mathcal{SE}}}^{rop-qcca}(\mathcal{A}), \quad (9)$$

where the right hand side is one-half the difference between the advantages of  $\mathcal{A}$  in the experiments  $\mathbf{Exp}_{\mathcal{SE}'}^{rop-qcca-b}(\mathcal{A})$  and  $\mathbf{Exp}_{\widetilde{\mathcal{SE}}}^{rop-qcca-b}(\mathcal{A})$  respectively.

To represent the actions of the oracles on the register  $Q_{\mathcal{A}}$  of the quantum adversary  $\mathcal{A}$ , it is convenient to split  $Q_{\mathcal{A}}$  in three sections, as follows. In the case of  $\widetilde{\mathcal{SE}}$ , the action of the encryption oracle is then given by

$$|m, x, y\rangle \longrightarrow |m, x \oplus c, y \oplus \tau\rangle, \quad (10)$$

where

$$c = \begin{cases} \mathcal{E}_{K_1}(m) & \text{if } b = 1, \\ \mathcal{E}_{K_1}(H(m)) & \text{if } b = 0, \end{cases} \quad (11)$$

and  $\tau = f(c)$ , and the action of the decryption oracle is given by

$$|x, c, \tau\rangle \longrightarrow |x \oplus \widetilde{\mathcal{D}}_{K_1}(c, \tau), c, \tau\rangle. \quad (12)$$

We can use a quantum adversary  $\mathcal{A}$  attacking the RoP-qsCCA security of  $\widetilde{\mathcal{SE}}$  to construct a quantum adversary  $\mathcal{B}$  attacking the RoP-qsCPA security of  $\mathcal{SE}$  using  $q_e$  encryption oracles queries. The quantum adversary  $\mathcal{B}$  runs  $\mathcal{A}$ , and uses its oracles to provide a simulation of  $\mathcal{A}$ 's oracles in the RoP-qsCCA experiment.  $\mathcal{B}$  simulates  $\mathcal{A}$ 's decryption queries by answering all of them with  $\perp$ . We need to link the advantages of  $\mathcal{A}$  and  $\mathcal{B}$ .

The main difficulty here is to derive a bound on the additional advantage of  $\mathcal{A}$  due to its ability to make decryption queries. In a classical (non-quantum) setting, since  $f$  is a true random function, the probability that an adversary forges a valid tag for a ciphertext would be  $q_d/2^{n_\tau}$ . A classical adversary therefore would get  $\perp$  almost every time in response to its decryption queries, which means that the decryption oracle would be essentially useless to the classical adversary. But because our adversary  $\mathcal{A}$  is able to make superposition queries, we have to work harder.

As in the classical proof, we will derive the required bound by considering a modified decryption oracle which always returns  $\perp$  in response to the quantum adversary's decryption queries, irrespective of the values of  $c$  and  $\tau$ . We will refer to the experiment with the modified oracle as *scenario Q0*, and to the original experiment as *scenario Q1*.

In scenario Q1, the decryption oracle returns  $\perp$  only if the tag is invalid. Similar to Eq. (8), the action of the decryption oracle is thus described by the unitary operator  $\mathbf{V}$  acting on a register state  $|x, c, \tau\rangle$  as follows:

$$\mathbf{V} |x, c, \tau\rangle = \begin{cases} |x \oplus \mathcal{D}_{K_1}(c), c, \tau\rangle & \text{if } f(c) = \tau, \\ |x \oplus \perp, c, \tau\rangle & \text{otherwise.} \end{cases} \quad (13)$$

The time evolution of the quantum adversary can then be written as

$$\mathbf{U}_{qd} \mathbf{V} \dots \mathbf{U}_2 \mathbf{V} \mathbf{U}_1 \mathbf{V} \mathbf{U}_0 |s\rangle , \quad (14)$$

followed by a binary measurement whose outcome is the guess  $b'$ . The input state  $|s\rangle$  is the result of some initialisation. The unitary operators  $\mathbf{U}_i$  describe the evolution of the adversary between decryption queries and include the actions of the encryption oracle. The probability of outcome  $b'$  depends on the bit  $b$  in the experiment. We will denote the probability that the outcome in scenario Q1 is  $b' = 1$  for the two cases  $b = 0$  and  $b = 1$  by  $\Pr^{Q1-0}(b' = 1)$  and  $\Pr^{Q1-1}(b' = 1)$ , respectively. We have then

$$\mathbf{Adv}_{\mathcal{SE}}^{rop-qscqa}(\mathcal{A}) = \text{Adv}^{Q1} = \Pr^{Q1-1}(b' = 1) - \Pr^{Q1-0}(b' = 1) , \quad (15)$$

where we have introduced the notation  $\text{Adv}^{Q1}$  for convenience.

The only difference in scenario Q0 is that the decryption oracle always returns  $\perp$ . We denote the action of the decryption oracle in this case by  $\tilde{\mathbf{V}}$ , which acts like this:

$$\tilde{\mathbf{V}} |x, c, \tau\rangle = |x \oplus \perp, c, \tau\rangle . \quad (16)$$

The time evolution of the quantum adversary in scenario Q0 is then given by

$$\mathbf{U}_{qd} \tilde{\mathbf{V}} \dots \mathbf{U}_2 \tilde{\mathbf{V}} \mathbf{U}_1 \tilde{\mathbf{V}} \mathbf{U}_0 |s\rangle , \quad (17)$$

again followed by a binary measurement whose outcome is the guess  $b'$ . We will denote the probability that the outcome in scenario Q0 is  $b' = 1$  for the two cases  $b = 0$  and  $b = 1$  by  $\Pr^{Q0-0}(b' = 1)$  and  $\Pr^{Q0-1}(b' = 1)$ , respectively. Since in scenario Q0 the decryption oracle always return  $\perp$ , it is not useful for the quantum adversary  $\mathcal{A}$ . This leads to a bound on the CPA advantage of the adversary  $\mathcal{B}$ :

$$\mathbf{Adv}_{\mathcal{SE}}^{rop-qscpa}(\mathcal{B}) \geq \text{Adv}^{Q0} = \Pr^{Q0-1}(b' = 1) - \Pr^{Q0-0}(b' = 1) , \quad (18)$$

where we have introduced the notation  $\text{Adv}^{Q0}$  again for convenience.

The key relation between the probabilities for scenarios Q0 and Q1 is provided by the following **claim**:

$$\Pr^{Q1-b}(b' = 1) \leq \Pr^{Q0-b}(b' = 1) + (1 + 2n_d^2) 2^{-n_\tau/4} , \quad (19)$$

independently of the value of the bit  $b$ . From inequality (19), together with the unproblematic assumption that  $\Pr^{Q0-b}(b' = 1) \leq \Pr^{Q1-b}(b' = 1)$ , we can deduce

$$\begin{aligned} & |\text{Adv}^{Q1} - \text{Adv}^{Q0}| \\ &= |\Pr^{Q1-1}(b' = 1) - \Pr^{Q1-0}(b' = 1) - (\Pr^{Q0-1}(b' = 1) - \Pr^{Q0-0}(b' = 1))| \\ &= |\Pr^{Q1-1}(b' = 1) - \Pr^{Q0-1}(b' = 1) - (\Pr^{Q1-0}(b' = 1) - \Pr^{Q0-0}(b' = 1))| \\ &\leq |\Pr^{Q1-1}(b' = 1) - \Pr^{Q0-1}(b' = 1)| + |\Pr^{Q1-0}(b' = 1) - \Pr^{Q0-0}(b' = 1)| \\ &\leq 2(1 + 2n_d^2) 2^{-n_\tau/4} . \end{aligned} \quad (20)$$

Together with Eqs. (9), (15) and (18), this implies

$$\mathbf{Adv}_{\mathcal{SE}}^{rop-qscpa}(\mathcal{B}) + 2 \cdot \mathbf{Adv}_F^{qprf}(\mathcal{J}) \geq \mathbf{Adv}_{\mathcal{SE}'}^{rop-qscpa}(\mathcal{A}) - 2(1 + 2q_d^2) 2^{-n_\tau/4}, \quad (21)$$

which proves the theorem.

All that remains to be done is therefore to prove the claim (19). We start by examining the expressions (14) and (17). Since, in general, the unitaries  $\mathbf{U}_i$  entangle the adversary's quantum register with its internal registers, one cannot assume that the quantum register is in a pure state during decryption queries. Denote by  $\mathcal{C}$  the set of all (classical) ciphertexts  $c$ . For any ciphertext  $c \in \mathcal{C}$ , define the projector

$$\text{Proj}_c = \sum_{m, \tau} |m, c, \tau\rangle\langle m, c, \tau| = I \otimes |c\rangle\langle c| \otimes I. \quad (22)$$

Denote by  $\rho_i^e$  the state of the quantum register after the  $i$ -th encryption query in scenario Q1. Let  $\mathcal{C}'$  be the set of all ciphertexts that do not result from any encryption query. That is,  $\mathcal{C}'$  is the set of ciphertexts that have zero weight in all encryption queries, i.e.,

$$\mathcal{C}' = \{c \in \mathcal{C} : \text{Tr}(\text{Proj}_c \rho_i^e) = 0, i = 1, \dots, q_e\}, \quad (23)$$

where  $\text{Tr}$  denotes the trace. We can now define the set  $\mathcal{C}_{\text{valid}}$  as the set of pairs  $(c, f(c))$  that do not result from any encryption query,

$$\mathcal{C}_{\text{valid}} = \{(c, f(c)) : c \in \mathcal{C}'\}. \quad (24)$$

Since

$$|\mathcal{C}_{\text{valid}}| = 2^{-n_\tau} |\mathcal{C}' \times \{0, 1\}^{n_\tau}|, \quad (25)$$

trying to guess  $\tau = f(c)$  given a ciphertext  $c \in \mathcal{C}'$  leads to a valid pair with very small probability. The results of the  $q_e$  encryption queries contain no information about the set  $\mathcal{C}_{\text{valid}}$ .

Now let  $\rho_i^d$  be the state of the quantum register before the  $i$ -th decryption query in scenario Q1, and define

$$\text{Proj}_{\text{valid}} = \sum_{(c, \tau) \in \mathcal{C}_{\text{valid}}} |c, \tau\rangle\langle c, \tau|. \quad (26)$$

We can now define  $W_{\text{val}, i}$  as the total weight of terms belonging to  $\mathcal{C}_{\text{valid}}$  in the  $i$ -th decryption query ( $i = 1, \dots, q_d$ ),

$$W_{\text{val}, i} = \text{Tr}(\rho_i^d \text{Proj}_{\text{valid}}). \quad (27)$$

This can be re-expressed as follows. Let  $|\psi_i^d\rangle$  be the state of the totality of the adversary's quantum registers immediately before the  $i$ -th decryption query in scenario Q1,

$$|\psi_i^d\rangle = \mathbf{U}_{i-1} \mathbf{V} \dots \mathbf{U}_1 \mathbf{V} \mathbf{U}_0 |s\rangle, \quad (28)$$

which can be expanded in the form

$$|\psi_i^d\rangle = \sum_{j,m,c,\tau} \lambda_{j,m,c,\tau} |j,m,c,\tau\rangle, \quad (29)$$

where  $j$  labels the computational basis states of all internal registers (i.e., all registers in addition to the register  $Q_A$ ). We then have

$$W_{\text{val},i} = \langle \psi_i^d | \text{Proj}_{\text{valid}} | \psi_i^d \rangle = \sum_{j,m,c} |\lambda_{j,m,c,f(c)}|^2 = 1 - \sum_{j,m,c,\tau \neq f(c)} |\lambda_{j,m,c,\tau}|^2. \quad (30)$$

The probability that a direct measurement after the  $i$ -th decryption query gives a string  $(c, \tau) \in \mathcal{C}_{\text{valid}}$  is then given by the expectation value  $\mathbf{E}(W_{\text{val},i})$ .

Now the optimal way of searching for a string  $(c, \tau) \in \mathcal{C}_{\text{valid}}$  is Grover's algorithm [7,10]. As long as  $i$  is less than the minimum number of queries required for Grover's algorithm to succeed with certainty (which is approximately  $\frac{\pi}{4}\sqrt{2^{n_\tau}}$ ), the best probability with which any quantum algorithm can find a string  $(c, \tau) \in \mathcal{C}_{\text{valid}}$  using  $i$  queries is exactly the probability  $\text{Pr}_{\text{Grover}}$  achieved by running Grover's algorithm with  $i$  queries [12,1]. That probability is equal to  $\text{Pr}_{\text{Grover}} = \sin^2((i + \frac{1}{2})\theta)$ , where  $\sin \frac{\theta}{2} = \sqrt{2^{-n_\tau}}$  [10]. To a very good approximation,

$$\text{Pr}_{\text{Grover}} = 4i^2 2^{-n_\tau}. \quad (31)$$

By measuring the quantum register after the  $i$ -th query and then stopping, the quantum adversary can find a string  $(c, \tau) \in \mathcal{C}_{\text{valid}}$  with probability  $\mathbf{E}(W_{\text{val},i})$ . Therefore we must have

$$\mathbf{E}(W_{\text{val},i}) \leq 4i^2 2^{-n_\tau} \quad (32)$$

for  $i = 1, \dots, q_d$ . What we actually need is a bound on the probabilities for  $\sqrt{W_{\text{val},i}}$ . For any random variable  $X \geq 0$ , we have  $\text{Var}(\sqrt{X}) \geq 0$  and thus  $\mathbf{E}(\sqrt{X}) \leq \sqrt{\mathbf{E}(X)}$ . Hence,

$$\mathbf{E}(\sqrt{W_{\text{val},i}}) \leq 2i 2^{-n_\tau/2}. \quad (33)$$

Now we want to compare the probability of outputting the guess  $b' = 1$  in scenario Q0 and the probability of outputting the guess  $b' = 1$  in scenario Q1. Let  $|\psi_i^d\rangle$  denote the state immediately before the  $i$ -th decryption query in scenario Q1 as before and, similarly, let

$$|\tilde{\psi}_i^d\rangle = \mathbf{U}_{i-1} \tilde{\mathbf{V}} \dots \mathbf{U}_1 \tilde{\mathbf{V}} \mathbf{U}_0 |s\rangle \quad (34)$$

denote the state immediately before the  $i$ -th decryption query in scenario Q0. Let us first compare the action of  $\mathbf{V}$  and  $\tilde{\mathbf{V}}$  on the state  $|\psi_i^d\rangle$  for some  $i$ :

$$\begin{aligned} \mathbf{V}|\psi_i^d\rangle &= \sum_{j,m,c,\tau \neq f(c)} \lambda_{j,m,c,\tau} \mathbf{V}|j,m,c,\tau\rangle + \sum_{j,m,c,\tau = f(c)} \lambda_{j,m,c,\tau} \mathbf{V}|j,m,c,\tau\rangle \\ &= \sum_{j,m,c,\tau \neq f(c)} \lambda_{j,m,c,\tau} |j,m \oplus \perp, c, \tau\rangle \\ &\quad + \sum_{j,m,c,\tau = f(c)} \lambda_{j,m,c,\tau} |j,m \oplus \mathcal{D}_{K_1}(c), c, \tau\rangle, \end{aligned} \quad (35)$$

and

$$\begin{aligned}
\tilde{\mathbf{V}} |\psi_i^d\rangle &= \sum_{j,m,c,\tau \neq f(c)} \lambda_{j,m,c,\tau} \tilde{\mathbf{V}} |j, m, c, \tau\rangle + \sum_{j,m,c,\tau = f(c)} \lambda_{j,m,c,\tau} \tilde{\mathbf{V}} |j, m, c, \tau\rangle \\
&= \sum_{j,m,c,\tau \neq f(c)} \lambda_{j,m,c,\tau} |j, m \oplus \perp, c, \tau\rangle \\
&\quad + \sum_{j,m,c,\tau = f(c)} \lambda_{j,m,c,\tau} |j, m \oplus \perp, c, \tau\rangle .
\end{aligned} \tag{36}$$

Putting these together and using Eq. (30) twice, we get the following for the fidelity of these two states:

$$\begin{aligned}
&\left| \langle \psi_i^d | \tilde{\mathbf{V}}^\dagger \mathbf{V} | \psi_i^d \rangle \right| \\
&= \left| \sum_{j,m,c,\tau \neq f(c)} |\lambda_{j,m,c,\tau}|^2 + \sum_{j,m,m',c} \lambda_{j,m',c,f(c)}^* \lambda_{j,m,c,f(c)} \langle m' \oplus \perp | m \oplus \mathcal{D}_{K_1}(c) \rangle \right| \\
&= \left| \sum_{j,m,c,\tau \neq f(c)} |\lambda_{j,m,c,\tau}|^2 + \sum_{j,m,c} \lambda_{j,m \oplus \mathcal{D}_{K_1}(c) \oplus \perp, c, f(c)}^* \lambda_{j,m,c,f(c)} \right| \\
&\geq \left| \sum_{j,m,c,\tau \neq f(c)} |\lambda_{j,m,c,\tau}|^2 \right| - \left| \sum_{j,m,c} \lambda_{j,m \oplus \mathcal{D}_{K_1}(c) \oplus \perp, c, f(c)}^* \lambda_{j,m,c,f(c)} \right| \\
&= 1 - W_{\text{val},i} - \left| \sum_{j,m,c} \lambda_{j,m \oplus \mathcal{D}_{K_1}(c) \oplus \perp, c, f(c)}^* \lambda_{j,m,c,f(c)} \right| \\
&\geq 1 - W_{\text{val},i} - \sqrt{\sum_{j,m,c} \left| \lambda_{j,m \oplus \mathcal{D}_{K_1}(c) \oplus \perp, c, f(c)} \right|^2} \sqrt{\sum_{j,m,c} \left| \lambda_{j,m,c,f(c)} \right|^2} \\
&= 1 - W_{\text{val},i} - \sqrt{W_{\text{val},i}} \sqrt{W_{\text{val},i}} \\
&= 1 - 2W_{\text{val},i} .
\end{aligned} \tag{37}$$

This implies that the trace distance [10] of these two states is bounded as

$$D\left(\mathbf{V} |\psi_i^d\rangle, \tilde{\mathbf{V}} |\psi_i^d\rangle\right) \leq \sqrt{1 - (1 - 2W_{\text{val},i})^2} \leq 2\sqrt{W_{\text{val},i}} . \tag{38}$$

Before the first decryption query, the states of the adversary in both scenarios Q0 and Q1 are identical,

$$|\psi_1^d\rangle = \mathbf{U}_0 |s\rangle . \tag{39}$$

Before the second decryption query, the states are

$$|\tilde{\psi}_2^d\rangle = \mathbf{U}_1 \tilde{\mathbf{V}} |\psi_1^d\rangle \quad \text{and} \quad |\psi_2^d\rangle = \mathbf{U}_1 \mathbf{V} |\psi_1^d\rangle , \tag{40}$$

respectively. Therefore, for the trace distance we have

$$D\left(|\psi_2^d\rangle, |\tilde{\psi}_2^d\rangle\right) = D\left(\mathbf{V} |\psi_1^d\rangle, \tilde{\mathbf{V}} |\psi_1^d\rangle\right) \leq 2\sqrt{W_{\text{val},1}} . \tag{41}$$

For arbitrary  $i > 0$ , the triangle inequality gives us

$$\begin{aligned}
D(|\psi_{i+1}^d\rangle, |\tilde{\psi}_{i+1}^d\rangle) &= D(\mathbf{U}_i \mathbf{V} |\psi_i^d\rangle, \mathbf{U}_i \tilde{\mathbf{V}} |\tilde{\psi}_i^d\rangle) \\
&= D(\mathbf{V} |\psi_i^d\rangle, \tilde{\mathbf{V}} |\tilde{\psi}_i^d\rangle) \\
&\leq D(\mathbf{V} |\psi_i^d\rangle, \tilde{\mathbf{V}} |\psi_i^d\rangle) + D(\tilde{\mathbf{V}} |\psi_i^d\rangle, \tilde{\mathbf{V}} |\tilde{\psi}_i^d\rangle) \\
&= D(\mathbf{V} |\psi_i^d\rangle, \tilde{\mathbf{V}} |\psi_i^d\rangle) + D(|\psi_i^d\rangle, |\tilde{\psi}_i^d\rangle) \\
&\leq 2\sqrt{W_{\text{val},i}} + D(|\psi_i^d\rangle, |\tilde{\psi}_i^d\rangle) .
\end{aligned} \tag{42}$$

By induction, it follows that

$$D(|\psi_{q_d}^d\rangle, |\tilde{\psi}_{q_d}^d\rangle) \leq 2 \sum_{i=1}^{q_d-1} \sqrt{W_{\text{val},i}} . \tag{43}$$

This implies that, for any measurement, the probabilities for  $b' = 1$  in both scenarios can not differ by more than the right-hand side of Eq. (43). Now the expectation of that quantity is

$$\begin{aligned}
\mathbb{E} \left( 2 \sum_{i=1}^{q_d-1} \sqrt{W_{\text{val},i}} \right) &= 2 \sum_{i=1}^{q_d-1} \mathbb{E} \left( \sqrt{W_{\text{val},i}} \right) \\
&\leq 2^{-n_\tau/2} 4 \sum_{i=1}^{q_d-1} i \\
&\leq 2q_d^2 2^{-n_\tau/2} .
\end{aligned} \tag{44}$$

Using the Markov inequality this implies, for any  $\xi > 0$ ,

$$\begin{aligned}
\Pr \left( 2 \sum_{i=1}^{q_d-1} \sqrt{W_{\text{val},i}} \geq \xi \right) &\leq \frac{1}{\xi} \mathbb{E} \left( 2 \sum_{i=1}^{q_d-1} \sqrt{W_{\text{val},i}} \right) \\
&\leq \frac{2}{\xi} q_d^2 2^{-n_\tau/2} .
\end{aligned} \tag{45}$$

That is, with probability at least  $1 - \frac{2}{\xi} q_d^2 2^{-n_\tau/2}$ , we have that

$$\Pr^{Q^{1-b}}(b' = 1) \leq \text{Prob}^{Q^{0-b}}(b' = 1) + \xi , \tag{46}$$

irrespectively of the value of the bit  $b$ . It follows that

$$\Pr^{Q^{1-b}}(b' = 1) \leq \Pr^{Q^{0-b}}(b' = 1) + \xi + \frac{2}{\xi} n_d^2 2^{-n_\tau/2} . \tag{47}$$

We can now choose  $\xi$  so that this has the most convenient form. One possibility is  $\xi = 2^{-n_\tau/4}$ , which leads to

$$\Pr^{Q^{1-b}}(b' = 1) \leq \Pr^{Q^{0-b}}(b' = 1) + (1 + 2n_d^2) 2^{-n_\tau/4} , \tag{48}$$

which establishes the claim (19). This completes the proof of the theorem.  $\square$



## References

1. A. Ambainis, “Quantum search algorithms”, SIGACT News **35**, 22–35 (2004).
2. D. J. Bernstein, J. Buchmann and E. Dahmen, *Post-Quantum Cryptography* (Springer, 2009).
3. M. Bellare, A. Desai, E. Jorjipii and P. Rogaway, “A Concrete Security Treatment of Symmetric Encryption: Analysis of the DES Modes of Operation”, Proceedings of 38th Annual Symposium on Foundations of Computer Science, pp. 394–403 (IEEE Press, 1997).
4. M. Bellare and C. Nampreppe, “Authenticated Encryption: Relations among Notions and Analysis of the Generic Composition Paradigm”, Advances in Cryptology – ASIACRYPT 2000, pp. 531–545 (Springer, 2000).
5. D. Boneh and M. Zhandry, “Secure Signatures and Chosen Ciphertext Security in a Post-Quantum World”, Advances in Cryptology – CRYPTO 2013, pp. 361–379 (Springer, 2013).
6. T. Gagliardoni, A. Hülsing and C. Schaffner, “Semantic Security and Indistinguishability in the Quantum World”, arXiv:1504.05255 (cs.CR) (2015).
7. L. K. Grover, “A fast quantum mechanical algorithm for database search”, Proceedings of the twenty-eighth annual ACM symposium on Theory of computing, pp. 212–219 (ACM, New York, 1996).
8. S. Hallgren, A. Smith and F. Song, “Classical cryptographic protocols in a quantum world”, Advances in Cryptology – CRYPTO 2011, pp. 411–428 (Springer, 2011).
9. J. Katz and Y. Lindell, *Introduction to Modern Cryptography*, (Chapman & Hall/CRC, 2007).
10. M. A. Nielsen and I. L. Chuang, *Quantum computation and quantum information* (Cambridge University Press, 2000).
11. D. Unruh, “Quantum proofs of knowledge”, Advances in Cryptology – EUROCRYPT 2012, pp. 135–152 (Springer, 2012).
12. C. Zalka, “Grover’s quantum searching algorithm is optimal”, Phys. Rev. A **60**, 2746–2751 (1999).